



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/454,865	12/07/1999	SHINICHIRO TANIGUCHI	104934	4339
25944	7590	08/23/2006	EXAMINER	
OLIFF & BERRIDGE, PLC P.O. BOX 19928 ALEXANDRIA, VA 22320			COLIN, CARL G	
			ART UNIT	PAPER NUMBER
			2136	

DATE MAILED: 08/23/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/454,865	TANIGUCHI ET AL.	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 30 May 2006.
- 2a) ☒ This action is FINAL. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-27 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-27 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>see att.</u> | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Information Disclosure Statement

1. The information disclosure statement filed 7/12/2006 fails to comply with the provisions of 37 CFR 1.97, 1.98 and MPEP § 609 because a translation is not provided for the Non-Patent publication "New Logistics System...". It has been placed in the application file, but the information referred to therein has not been considered as to the merits. Applicant is advised that the date of any re-submission of any item of information contained in this information disclosure statement or the submission of any missing element(s) will be the date of submission for purposes of determining compliance with the requirements based on the time of filing the statement, including all certification requirements for statements under 37 CFR 1.97(e). See MPEP § 609.05(a).

Response to Arguments

2. In response to communications filed on 5/30/2006, the following claims 1-27 are presented for examination.

2.1 Applicant's arguments, see pages 1-11, filed on 5/30/2006, with respect to the rejection of claims 1-27, have been fully considered, but they are not persuasive. Regarding claim 1, Applicant argues that the control and monitoring unit of Bauer cannot reasonably be considered to correspond to a data carrier attached to an article that stores information relative to the article, the data carrier being an electronic tag, because the control and monitoring unit of Bauer has a

Art Unit: 2136

computer with data and program memories in addition to other features. Examiner respectfully disagrees. First the electronic tag as defined in Applicant's disclosure is merely a data carrier. Applicant's disclosure, page 3 recites, "To exclude such a fraudulent practice, a modified method in which the information is stored together with a signature in an electronic tag (data carrier) has been proposed. An electronic tag is referred to as a data carrier hereinafter". Applicant's background clearly admits that a data carrier or electronic tag attached to an article that stores information relative to the article has been well known in the art. Bauer also discloses in column 1, that these are well known features and further discloses way of improving risk and liability in a transport system using a data carrier by having a continuous monitoring and control of the merchandise from the manufacturer to the final destination in such a manner that only authorized persons by way of coding can obtain access to all units; and the party responsible for the transport can read out and document the data stored in the data carrier up to the point in time of delivery as a proof of the party's performance; it is desirable that uninterrupted proof be maintained concerning the course of transport (see Bauer's summary of invention). In response to Applicant's reply that there is no suggestion of a data carrier attached to an article that stores information relative to the article, Bauer discloses "a control and monitoring unit firmly connected with the good (article) to be distributed and accompanies the good with the transport momentary state is recorded, stored, and possibly displayed" (column 2, lines 10-25). In response to Applicant's argument that "it is difficult to understand how a memory card can comprise a computer and a memory card cannot reasonably be considered to comprise a computer", Examiner would like to clarify for Applicant that a computer is a device that computes and a memory card comprises this functionality. In response to Applicant's argument

Art Unit: 2136

that the smartcard of Sudia cannot reasonably perform signature generating process because it cannot correspond to a signature module, Examiner respectfully disagrees (see Sudia's summary). Examiner asserts that Sudia discloses signing devices and smart card as an example of signing device and clearly discloses a smart card that affix signatures and participates in signature generating process as shown at least in the paragraphs below:

[0046] Groups of authorizing agents 23, 25, 27, 29, 31 are also interconnected through the network to one another and to the signing devices 11, 13, 15, 17, 19. Each authorizing agent is a person acting through a trusted computer device (such as a tamper-resistant smart card, or other trusted device) as will be discussed more fully below.

[0057] The signing device previously shown in FIG. 2 may also be a smart card having the same general design as the trusted devices of the authorizing agents.

[0054] FIG. 3 illustrates a working station for authorizing agents. The human operators who act as authorizing agents may work in relatively unsecured areas at desk-top computers or terminals 51 typically found in a business office. Each such computer or terminal will have a card reader 53, and each operator will have a secure "smart card" 55. Each smart card 55 securely contains a private decryption key and a private signature key which are unique to that smart card. The human operator can use the card to issue signing instructions. Such a trusted device may be implemented using a FIPS level-3 device, such as an Power card from National Semiconductor Corp. of Santa Clara, Calif., which can be readily reprogrammed at the firmware level to allow for progressive evolution of new methods and procedures for secure signing and authorization without needing to replace the physical devices. Each authorizing agent's trusted device must have at least a private signature key. Preferably, the private signature key is installed in the device at time of manufacturer, and the corresponding public verification key is "certified" by the manufacturer. Certification here means that the manufacturer has included, with the trusted device, an electronic message containing the device's serial number and public key, along with its model number and other evidence of its trusted characteristics, and that message (certificate) has been signed by the manufacturer.

[0055] The human operators use their desk-top computers to read and generate messages. When a human operator wishes to sign a message, the desk-top computer sends the message to the trusted device, which appends a digital signature using the device private signature key. In the preferred embodiment, this signature is the signature of a second signature key pair which has been specifically generated for and certified as belonging to the specified user. In this manner, the system can continue to use the device's signature to verify the trust level of the device on any given transaction, while using the user's signature to attest to the user's identity and consent to the transaction. This allows the user key to be generated and revoked remotely, depending possibly on various administrative facts about the user's identity or authority, while also allowing the device to be reused, or to host several other user key pairs which the user may wish to use for other unrelated purposes.

Applicant generally alleges that the prior art does not teach the claimed limitation of claim 1 without showing how the citations provided in the Office Action do not disclose the claimed limitation as claimed. For instance, Applicant argues that Bauer does not disclose that the memory card verifies information relative to the goods; it only verifies identity of person

Art Unit: 2136

seeking access. As cited in the Office action, column 6, lines 7-8 recite that the identification code also comprises type of merchandise destination address, name of the originator and addressee... owner of the transported goods all this information meets the recitation of information that relates to the goods and the memory card comprises access coding for verification (see column 6, lines 25-37). Applicant also argues that the analysis unit that meets the recitation of information generating unit does not communicate with (1) and does not process information to be stored in (1). Examiner respectfully disagrees (see figure 1 and column 6, lines 25-55). In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., a system that documents the number of uses of an individual signature key as applied to an item and further limits the number of times an individual signature key can be applied to that item) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). In response to applicant's argument that Sudia's reference is nonanalogous art, it has been held that a prior art reference must either be in the field of applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the applicant was concerned, in order to be relied upon as a basis for rejection of the claimed invention. See *In re Oetiker*, 977 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992). In this case, Applicant is concerned of using signatures in a distribution process so as to verify the signatures of the signers during the distribution process. Sudia's reference among many other features discloses a signing system using signature tracking in managing a flow of an item and during the distribution process, each signer is able to verify other signers' signatures as well as

Art Unit: 2136

keeping track of the number of signatures (see page 14, paragraphs 229-234 and page 3, paragraph 44). In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). However, upon further consideration, applicant has not overcome the rejection as illustrated above. Claims 1-27 remain rejected in view of the same references.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3.1 **Claims 1-27** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,117,096 to **Bauer et al.** in view of US Patent Publication US 2002/0013898 to **Sudia et al.**

3.2 **As per claim 1, Bauer et al.** substantially teaches a distribution information management system having a structure comprising a control and monitoring unit connected with the goods to be distributed with sensors and actuators for storing state of distribution process that meets the

Art Unit: 2136

recitation of a data carrier attached to an article that stores information relative to the article, the data carrier being an electronic tag (see column 2, lines 10-24),

a distribution information processing module (3) comprising:

quick look unit (51) and interface (31) as input/output circuit for data reading in or out of the control monitoring unit that meets the recitation of a reading part and storing part that reads out data of the data carrier and stores information in the data carrier, for example (see column 6, lines 18-25);

an information generating unit (41) that processes the information to be stored in the data carrier wherein the information includes at least a signer identifier that is a receiver identifier of last information stored in the data carrier, for example (see column 2, lines 25-28; column 5, line 66 through column 6, line 15 and column 5, lines 9-21);

communication lines for communication between (2) and (4) or (3) and (4) that meets the recitation of a first communication part that communicates with the distribution information management module (4) (see figure 1) (see also column 6, lines 33-37);

a memory card (2), (first information verification unit) comprising:

a computer (32), (first verification part), for read write access and suggests using access code that meets the recitation of a first information verification unit comprising a first verification part that verifies the information read out from the data carrier a first verification key storage part (33 and 34) that stores the verification key used by the first information verification part for verification of the information, for example (see column 2, lines 15-25 and column 6, lines 1-55);

an information generating unit (41) that processes the information to be stored in the data carrier comprising: distribution information generating part (44) that generates the information to be stored in the data carrier (see column 2, lines 24-38 and column 6, lines 38-65).

Bauer et al. discloses a programmable card as well as an analysis unit for verifying all transactions during the distribution process, for example (see column 2, line 47 through column 3, line 35) and discloses each unit comprising computer and interfacing with the memory card and capable of interfacing with each other (see figure 1). Although **Bauer et al.** discloses some security with access code etc., **Bauer et al.** does not explicitly disclose a signature generating process that stores signature key information for generating a digital signature. However, **Sudia et al** in an analogous art discloses a distribution verification system that is able to sign and verify the signature of the sender comprising first verification key storage part that stores the verification key used by the first information verification part for verification of the information, for example (see page 3, paragraphs 44-45, 0047-0048; page 5, paragraph 72; page 6, paragraph 78), a signature module that performs signature generating process, for example (see page 4, paragraph 0054); a signature key storage part that stores the signature key information used by the signature module for generating a digital signature, for example (see page 4, paragraphs 0054-0055); **Sudia et al** discloses that each signing device and each authorizing agent has set of public and signature verification keys of other devices (page 5, paragraph 0066), and suggests that keys will be selected or acquired from the stored keys (page 4, paragraph 0050) that meets the recitation of a signature key information selection part; that selects a signature key information stored in the signature key storage part; a signature key information acquisition part that acquires the signature key information from the distribution information management

Art Unit: 2136

module, for example (see page 4, paragraph 0050); the signature module comprising: a signature part that generates a digital signature for the information generated by the distribution information generating part, for example (see page 4, paragraphs 0054-0055); and a first signer private information storage part that stores signer private information used by the signature part for generating a digital signature, for example (see page 4, paragraphs 0054-0055); **Sudia et al** discloses assigning or including in the header of each document a document and signature tracking to assist in managing the flow of documents through the system comprising the total number of partial signatures needed to complete the signature and the number of partial signatures already applied (see page 14, paragraphs 229-234) that meets the recitation of a signature key use limit information storage part that stores a signer key use limit information to indicate whether the signature key information is already used. **Sudia et al** suggests interaction between devices and a signature key information generating part that generates a signature key information used by the distribution information processing module, for example (see page 5, paragraphs 0067-0072). **Sudia et al** adds that the verification process disclosed offers several advantages in preventing tampering (page 4, paragraph 0053) including applying a signature and at the same time verifying the signature of the sender and with improved security and flexibility (see page 1, paragraphs 0006 and 0012). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of **Bauer et al.** to provide a key signature verification process as taught by **Sudia et al** capable of generating, storing, selecting key, and verifying signature of the sender. One of ordinary skill in the art would have been motivated to do so because **Sudia et al** teaches many advantages as explained below to implement a multi-step signing system, when plurality of signatures are needed from

Art Unit: 2136

authorized agents that are widely dispersed (par. 6 and 43). The motivation to do so is given by **Sudia et al** who teaches a multi-step signing system wherein the signing module provided for verifying signature of other signers for performing, generating and distributing keys is a tamper-proof secure signing device; security of the system is enhanced by distributing capability to affix signatures among a plurality of signing devices, the system can use the signature of the device to verify the trust level of the device on any given transaction; Sudia et al further teaches, no single signing device or location needs to contain the signature key where it can be compromised instead multiple sites must fail or compromise together; the system is both secure and flexible because if any signing device fails it can be replaced, security is enhanced as the signing operation cannot be completed with a single signing device (see page 2, paragraphs 12-15).

Bauer et al. discloses communication lines for communication between (2) and (4) or (3) and (4) that meets the recitation of a first communication part that communicates with the distribution information management module (4) (see figure 1); and further discloses the distribution information management module (4) comprising: interface that meets the recitation of a second communication part that communicates with the distribution information processing module, for example (see column 6, lines 35-50);

Bauer et al. discloses a programming unit capable of programming information and access codes in the control and monitoring unit (1) and a memory card (2) and processing and verifying information (column 4, line 66 through column 5, lines 37) that meets the recitation of second information verification part that verifies the information received from the distribution information processing module; other unit such as (61) that may be connected to (4) may perform similar process for example (see column 6, lines 32-65).

Sudia et al discloses signing device and authorizing agent that can perform the same function as discussed above (see page 5, paragraph 0057); therefore, **Sudia et al** also discloses a second verification key storage part that stores the verification key used by the second information verification part for verification of the information (see page 5, paragraph 0066); a signature key information generating part that generates a digital signature key information used by the distribution information processing module for generating a distribution information, for example (see page 5, paragraph 0069); a signature key storage part and a signer private information selection part that selects signer private information used by the signature key information generating part for generating signature key information (see page 4, paragraphs 0054-0055); and a second signer private information storage part that stores the signer private information (see page 5, paragraphs 0066 and 0072). Therefore, it would have been obvious to one skilled in the art at the time the invention was made to modify the system of **Bauer et al.** to provide a second key signature verification unit as taught by **Sudia et al** capable of generating, storing, selecting key, and verifying signature of the sender. One of ordinary skill in the art would have been motivated to do so because **Sudia et al** teaches many advantages as explained below to implement a multi-step signing system, when plurality of signatures are needed from authorized agents that are widely dispersed (par. 6 and 43). The motivation to do so is given by **Sudia et al** who teaches a multi-step signing system wherein the signing module provided for verifying signature of other signers for performing, generating and distributing keys is a tamper-proof secure signing device; security of the system is enhanced by distributing capability to affix signatures among a plurality of signing devices, the system can use the signature of the device to verify the trust level of the device on any given transaction; **Sudia et al** further teaches, no single

signing device or location needs to contain the signature key where it can be compromised instead multiple sites must fail or compromise together; the system is both secure and flexible because if any signing device fails it can be replaced, security is enhanced as the signing operation cannot be completed with a single signing device (see page 2, paragraphs 12-15).

As per claims 2-3, both references suggest using a smart card for verification process that can be detachable from other units. **Sudia et al** discloses using a smart card that is tamperproof that meets the recitation of wherein the signature module is tamperproof and detachable from the distribution information processing module (see page 4, paragraphs 0054-0055). Therefore, claim 2 is rejected on the same rationale as the rejection of claim 1.

As per claim 4, **Bauer et al.** discloses the claimed system of claim 1 but does not disclose the limitation wherein the information generating unit has a signature key use limit information storage part that limits a specified number times for signatures performed using the signature key; the signature key information selection part does not select signature key information used more than a specified number of times for signature. It is well known in the art program that limits and revokes number of times of performing password or using keys. **Sudia et al** discloses limiting use of key signature and key revocation that meets the recitation of a signature key use limit information storage part that limits a specified number times for signatures performed using the signature key, the signature key information selection part does not select signature key information used more than a specified number of times for signature, for example (see page 5, paragraphs 0056, and page 6, paragraph 0075, and page 7, paragraphs

Art Unit: 2136

0014-0115 and page 13, paragraph 0197). Therefore it would have been obvious to one skilled in the art at the time the invention was made to modify the system of **Bauer et al.** to limit a specified number times for signatures performed using the signature key, not selecting signature key information used more than a specified number of times for signature as suggested by **Sudia et al.** This modification would have been obvious because one skilled in the art would have been motivated to do so in order to protect keys from susceptible attacks as suggested by **Sudia et al** (see page 7, paragraphs 0014-0115).

As per claim 5, **Sudia et al** discloses the limitation of wherein the signature key use limit information storage part is disposed in the signature module (see page 7, paragraphs 0014-0115). Therefore, claim 5 is rejected on the same rationale as the rejection of claim 4.

Claim 6 has the same limitation as claim 1 except for adding a second reading and storage part in the information generating module. **Bauer et al.** discloses more than one unit with reading/writing means to read and store the information in the data carrier (see column 2, lines 10-40 and column 3, lines 25-45 and column 4, lines 1-12).

Claim 7 has the same limitation as the rejected claim 1 except for adding a third communication part. **Bauer et al.** discloses many interfaces between the units (see figure 1). Therefore, **claim 7** is rejected on the same rationale as the rejection of **claim 1**.

As per claim 8, Sudia et al discloses the limitation of wherein the verification key stored in the first verification key storage part and the second verification storage part is common for all the distribution information processing modules and distribution information modules, for example (see page 3, paragraph 0048). Therefore, **claim 8** is rejected on the same rationale as the rejection of **claim 1**.

As per claim 9, Sudia et al discloses signing device and authorizing agent that can perform the same function as discussed above (see page 5, paragraph 0057).

As per claims 10-12, Sudia et al discloses that each signing device and each authorizing agent has set of public and signature verification keys of other devices (page 5, paragraph 0066), and suggests that keys will be selected or acquired from the stored keys (page 4, paragraph 0050). These claims are therefore rejected on the same rationale as the rejection of claim 1 above.

As per claim 13, Bauer et al. discloses the limitation wherein the information stored in the data carrier comprises at least a product identifier, an identifier of a receiver at a destination of the article and access coding, and which information is stored as one unit (see column 6, lines 1-25 and column 4, line 67 through column 5, line 22). **Bauer et al.** does not explicitly disclose a signature value, but discloses using a data carrier for documenting the originator or addressee and the transfer of responsibility for the transport and control operations during the whole course of distribution (column 2, lines 46-67). However, **Sudia et al** discloses appending signature

value to verify the sender, for example (see page 4, paragraph 0055). Therefore it would have been obvious to one skilled in the art at the time the invention was made to modify the system of **Bauer et al.** to add a signature value to the data carrier so as to authenticate the originator or sender and to prevent tampering. This modification would have been obvious because one skilled in the art would have been motivated to do so in order to have further control of authorization during the distribution process as suggested by **Sudia et al** (see page 1, paragraph 0012).

As per claim 14, Bauer et al. suggests maintaining proof concerning the course of the transport and discloses a data carrier for holding all information during the course of the distribution process for replacing transport papers (see column 2, lines 47-60 and column 1, lines 49-62). **Sudia et al** discloses the limitation of wherein the information stored in the data carrier contains at least a verification key identifier, and which information is stored as one unit (see page 6, paragraph 0078). Therefore claim 14 is rejected on the same rationale as the rejection of claims 1 and 13.

As per claim 15, Bauer et al. discloses the limitation wherein the information stored in the data carrier contains at least a distribution information management module identifier, and which information is stored as one unit (see column 6, lines 1-12).

As per claim 16, Bauer et al. discloses the limitation wherein the information stored in the data carrier as one unit contains at least a product identifier, an identifier of a receiver at a

Art Unit: 2136

destination of the article and access coding that can be separately from the information for unit.

Bauer et al discloses a data carrier with different units, it is obvious to one skilled in the art that the signature value can be stored separately from the other information. (see column 6, lines 1-12 and lines 25-37). **Sudia et al** discloses using signature value to verify the sender, for example (see page 4, paragraph 0055) as discussed in claim 13 above. Claim 16 is rejected on the same rationale as the rejection of claims 1 and 13.

As per claim 17, Bauer et al. discloses the limitation wherein the information stored in the data carrier contains at least a product identifier, an identifier of a receiver at a destination of the article and a verification key identifier and which information is stored as one unit, and identification code that indicates each verifier that meets the recitation of the information has a signature value corresponding to the verification key identifier for each verification identifier (see column 3, lines 9-26 and column 5, lines 1-11; column 5, line 65 through column 6, line 37). **Bauer et al.** discloses continuous proof and monitoring throughout the transport (see column 1, lines 49 et seq. and column 2, lines 15-24). **Sudia et al** discloses wherein the information stored in the data carrier contains at least a product identifier, an identifier of a receiver at a destination of the article and a verification key identifier and which information is stored as one unit, and the information has a signature value corresponding to the verification key identifier for each verification identifier (see page 6, paragraph 0078). Claim 17 is rejected on the same rationale as the rejection of claims 1 and 13.

As per claim 18, Bauer et al. discloses a data carrier attached to an article for storing information of the article that stores (see column 4, lines 46 et seq.): distribution information generated for each one or one set of transaction in the distribution process of the article, wherein the distribution information includes at least a signer identifier that is a receiver identifier of last information stored in the data carrier; and at least a part of a signature value of at least part of a piece of the distribution information or at least part of each of serial pieces of the distribution information (see column 5, lines 1-22 and column 5, line 65 through column 6, line 37). Claim 18 contains similar limitation as claims 1 and 13 and therefore is rejected on the same rationale as the rejection of claims 1 and 13.

As per claim 19, Bauer et al. discloses the limitation wherein the distribution information of the article contains at least an identifier of the article, an identifier of the receiver who received the article, and identification code that indicates each verifier that meets the recitation of identifier of the signer who generates the signature value (see column 5, line 65 through column 6, line 37). **Sudia et al** discloses an identifier of the receiver who received the article, and the identifier of the signer who generates the signature value (see page 6, paragraphs 0078 and 0080) as discussed in claim 13.

Claims 20-23 are similar to the rejected claim 1 except for incorporating the claimed system into a module and a method. Therefore, **claims 20-23** are rejected on the same rationale as the rejection of claim 1.

Claims 24-25 have the same limitation as the rejected claim 1 except for incorporating the claimed system into a computer program product. Therefore, **claims 26-27** are rejected on the same rationale as the rejection of claim 1.

Claims 26-27 have the same limitation as the rejected claim 1. Therefore, **claims 26-27** are rejected on the same rationale as the rejection of claim 1.

Conclusion

4. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

4.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

Art Unit: 2136

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.


cc

Carl Colin

Patent Examiner

August 18, 2006

NASSER MOAZZAM
PRIMARY EXAMINEE


8,18,06